TimestampServer

utimaco®

Secure timestamps for document and data authenticity

The Utimaco TimestampServer is the ideal Hardware Security Module (HSM) for business applications that require proving the **existence and status of a document or data** at a **specific point in time**.

It ensures the **tamper-proof creation and authenticity of timestamps** for electronic contracts, the reception of offers on electronic tender platforms or the submission time of a bet to an online lottery game. The Utimaco TimestampServer ensures that timestamped data is authentic for these and similar applications. It is able to verify at all times, whether or not the timestamped data matches the exact same form at the point in time it was logged by the timestamp.

Regular re-creation of a **current timestamp guarantees continuity** of the audit trail. This enables long-term archiving – year after year, even after the expiration of older signature certificates.

The TimestampServer is only available as network appliance.

Contact
hsm@utimaco.com
hsm.utimaco.com

EMEA
Utimaco IS GmbH – Headquarters
Germanusstraße 4
52080 Aachen, Germany
Phone +49 241 1696 200

Americas
Utimaco Inc.
910 E Hamilton Ave., Suite 150
Campbell, CA 95008, USA
Phone +1 844 UTIMACO

APAC
Utimaco IS GmbH – Office APAC
One Raffles Quay, North Tower, Level 25
Singapore 048583
Phone +65 6622 5347

Fields of application

- Document management and archiving systems
- Long-term archiving solutions
- Electronic tender platforms
- Lottery and online betting
- Electronic contracts
- Support and ticketing systems

Secure investment

- Highest performance level at an attractive price
- Non-limited number of connections
- Easy software upgrades for adapting to future timestamp protocols and algorithms

Interfaces

- RFC 3161 timestamp protocol via HTTP or TCP, IPv4 and IPv6 network protocol
- CryptoServer Timestamp API for general TimestampServer administration
- PKCS#10 and PKCS#7 for request and import of TimestampServer certificates
- Network Time Protocol (NTP) for synchronization of TimestampServer with external time server

Algorithms

- RSA, key length up to 8192 bits
- Hash algorithms SHA-1, SHA-2 family, SHA-3, RIPEMD-160, MD5

Security

- Integrated Hardware Security Module is certified in accordance with FIPS 140-2 Level 3
- FIPS 140-2 Level 4 physical security with TimestampServer CSe-Series
- Meets requirements of ETSI Technical Specification TS102023 “Policy Requirements for Timestamping Authorities”

Specifications and technical data

- 19” 1U form factor
- Redundant field-replaceable power supply: 2 x 100 ~ 240 V AC, 50 ~ 60 Hertz, 300 W
- Power consumption: typically 45 W / 66 VA, max. 50 W / 70 VA
- Heat dissipation: max. 171 BTU/h
- 2 RJ45 1 Gb/s network interfaces
- Operating temperature TimestampServer Se Gen2-Series: +10°C to +50°C (+50°F to +122°F)
- Operating temperature TimestampServer CSe-Series: +10°C to +40°C (+50°F to +104°F)
- Storage temperature: -10°C to +55°C (+14°F to +131°F)
- Relative humidity: 10% to 95%, non-condensing
- MTBF 100,000 hours at 25°C / 77°F, environment GB, GC – Ground Benign, Controlled